Verschlüsselungsverfahren zum Ausführen von kryptographischen Operationen

Patent number: DE19936890

Publication date: 2000-04-06

Inventor: PHILIPP STEFAN (DE)

Applicant: PHILIPS CORP INTELLECTUAL PTY (DE)

Classification:

- international: G06F12/14; G06K19/073; H04L9/20

- european: G06F1/00N1C, G06F21/00N1C1, G06F21/00N1C4, H04L9/06C

Application number: DE19991036890 19990805

Priority number(s): DE19991036890 19990805; DE19981045096 19980930

Also published as:

WO0019657 (A1)

EP1044534 (A1)

Abstract of **DE19936890**

The invention relates to an encoding method according to which a partial cryptographic operation is carried out by data which are digitally stored as at least one data bit word in a memory cell (1) or a register. To provide such a system which effectively prevents successful cryptanalysis by observation of a current consumption of a data processing unit, the invention provides for a data bit word generated on the basis of random numbers to be stored in a memory cell (10) before a data bit word is written into same.

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 199 36 890 A 1**

(51) Int. Cl.[7]:
G 06 F 12/14
G 06 K 19/073
H 04 L 9/20

(21) Aktenzeichen: 199 36 890.2
(22) Anmeldetag: 5. 8. 1999
(43) Offenlegungstag: 6. 4. 2000

DE 199 36 890 A 1

(66) Innere Priorität:
198 45 096. 6 30. 09. 1998

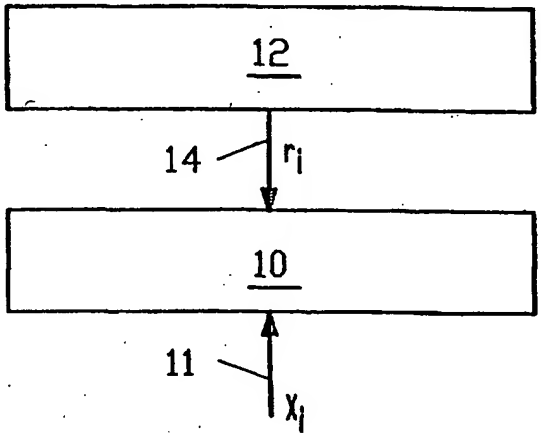
(71) Anmelder:
Philips Corporate Intellectual Property GmbH, 22335 Hamburg, DE

(72) Erfinder:
Philipp, Stefan, 20259 Hamburg, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Verschlüsselungsverfahren zum Ausführen von kryptographischen Operationen

(57) Um ein Verschlüsselungsverfahren, bei dem eine kryptographische Teiloperation von digital als wenigstens ein Datenbitwort in einer Speicherzelle (10) bzw. einem Register gespeicherten Daten ausgeführt wird, zur Verfügung zu stellen, welches eine erfolgreiche Kryptoanalyse mittels Beobachtung eines Stromverbrauches eines Datenverarbeitungsgerätes wirksam verhindert, wird vorgeschlagen, dass vor dem Schreiben eines Datenbitwortes in eine Speicherzelle (10) in dieser ein Datenbitwort gespeichert wird, welches auf Zufallszahlen basierend erzeugt wird.



DE 199 36 890 A 1

Beschreibung

Technisches Gebiet

Die Erfindung betrifft ein Verschlüsselungsverfahren, wobei wenigstens eine kryptographische Teiloperation von digital als wenigstens ein Datenbitwort in einer Speicherzelle bzw. einem Register gespeicherten Daten ausgeführt wird, gemäß dem Oberbegriff des Anspruchs 1.

Stand der Technik

In vielen Datenverarbeitungsgeräten dienen kryptographische Operationen zum Schutz des Betriebes dieser Geräte bzw. zum Schutz von in dem Gerät transportierte Daten. Die hierfür notwendigen Berechnungsoperationen werden dabei sowohl von Standard-Rechenwerken als auch von dedizierten Crypto-Rechenwerken durchgeführt. Ein typisches Beispiel für letzteres sind Chipkarten bzw. IC-Karten. Bei derartigen kryptographischen Berechnungen ist es oftmals notwendig, entsprechende Speicherbereiche bzw. Register des Datenverarbeitungsgerätes mit Operanden zu initialisieren. Bei den in diesem Zusammenhang verwendeten Daten bzw. Zwischenergebnissen handelt es sich üblicherweise um sicherheitsrelevante Informationen, wie beispielsweise kryptographische Schlüssel oder Operanden.

Zur Berechnung der kryptographischen Algorithmen werden in den Datenverarbeitungsgeräten logische Verknüpfungen zwischen Operanden bzw. Zwischenergebnissen durchgeführt. In Abhängigkeit von der verwendeten Technologie führen diese Operationen, insbesondere das Laden von leeren oder zuvor gelöschten Speicherbereichen bzw. Register mit Daten, zu einem erhöhten Stromverbrauch der Datenverarbeitungsgeräte. Bei komplementärer Logik, wie beispielsweise der CMOS-Technik, tritt ein erhöhter Stromverbrauch dann auf, wenn der Wert einer Bit-Speicherzelle geändert wird, d. h. sein Wert sich von "0" auf "1" bzw. von "1" auf "0" ändert. Der erhöhte Verbrauch hängt dabei von der Anzahl der im Speicher bzw. Register geänderten Bitstellen ab. Mit anderen Worten lässt das Laden eines zuvor gelöschten Registers einen Stromverbrauch proportional zum Hamminggewicht des in das leere Register geschriebenen Operanden (= Anzahl der Bits mit dem Wert "1") ansteigen. Durch eine entsprechende Analyse dieser Stromänderung könnte es möglich sein, Informationen über die berechneten Operationen zu extrahieren, so dass eine erfolgreiche Kryptoanalyse von geheimen Operanden, wie beispielsweise kryptographischen Schlüsseln, möglich ist. Mittels Durchführung mehrerer Strommessungen am Datenverarbeitungsgerät könnten beispielsweise bei sehr kleinen Signaländerungen eine hinreichende Extraktion der Informationen ermöglicht werden. Andererseits könnten mehrere Strommessungen eine ggf. erforderliche Differenzbildung ermöglichen. Diese Art der Kryptoanalyse wird auch als "Differential Power Analysis" bezeichnet, mittels derer ein Außenstehender durch reine Beobachtung von Änderungen des Stromverbrauches des Datenverarbeitungsgerätes eine ggf. unberechtigte Kryptoanalyse der kryptographischen Operationen, Algorithmen, Operanden bzw. Daten erfolgreich ausführen kann.

Bei einer aus der EP 0 482 975 B1 bekannten Speicherkarte mit Mikroschaltung und wenigstens einem Speicher, die an einem Datenverarbeitungsorgan angeschlossen ist, wobei das Datenverarbeitungsorgan von einem Datensignal von außerhalb der Karte gesteuert wird und als Antwort auf dieses Datensignal zu einem Zeitpunkt ein Befehlsendesignal abgibt, welches um eine vorbestimmte Dauer (T) bzgl. des Empfangs des Datensignals verzögert ist, wird zum Erhöhen des Schutzes die Zeitdauer (T) auf Zufallsbasis zeitlich variabel gewählt. Eine Kryptoanalyse auf der Basis einer Stromänderung beim Beschreiben des Speichers kann dieses System jedoch nicht verhindern.

Darstellung der Erfindung, Aufgabe, Lösung, Vorteile

Es ist Aufgabe der vorliegenden Erfindung, ein verbessertes Verfahren der obengenannten Art zur Verfügung zu stellen, welches die obengenannten Nachteile beseitigen und eine erfolgreiche Kryptoanalyse mittels Beobachtung eines Stromverbrauches eines Datenverarbeitungsgerätes wirksam verhindert.

Diese Aufgabe wird durch ein Verfahren der o. g. Art mit den in Anspruch 1 gekennzeichneten Merkmalen gelöst.

Dazu ist es erfindungsgemäß vorgesehen, dass vor dem Schreiben eines Datenbitwortes in eine Speicherzelle in dieser ein Datenbitwort gespeichert wird, welches auf Zufallszahlen basierend erzeugt wird.

Dies hat den Vorteil, dass eine nicht vorbestimmte oder vorbestimmbare Vorinitialisierung vorliegt, welche aus Änderungen des Stromverbrauches beim Schreiben in die Speicherzelle keinen Rückschluß auf das in die Speicherzelle geschriebene Datenbitwort zulässt. Beim Einschreiben von Daten in derartig vorinitialisierte Speicherzellen ändert sich der Stromverbrauch lediglich abhängig von einer Differenz des Hamminggewichtes der eingeschriebenen Daten von der unbekannten Zufallszahl, so daß auch diese Differenz und damit die Änderung des Stromverbrauches zufällig und nicht vorherbestimmbar ist.

Bei der Umsetzung des Verfahrens bestehen verschiedene Möglichkeiten. Nach einer bevorzugten Vorgehensweise wird das auf Zufallszahlen basierende Bitwort von einem Rechenwerk in die Speicherzelle geschrieben. Alternativ wird das auf Zufallszahlen basierende Bitwort über eine direkte Verbindung zwischen einer Zufallszahlenquelle und der Speicherzelle in letztere geschrieben.

Eine zeitliche Korrelation zwischen dem Einschreiben der Zufallszahl in eine Speicherzelle und der kryptographische Teiloperation wird dadurch vermieden, dass das auf Zufallszahlen basierende Bitwort zeitlich beabstandet vor der kryptographische Teiloperation in der Speicherzelle gespeichert wird.

Kurze Beschreibung der Zeichnungen

Nachstehend wird die Erfindung anhand der beigefügten Zeichnungen näher erläutert. Diese zeigt in der einzigen Figur ein Ablaufschema einer bevorzugten Ausführungsform eines erfindungsgemäßen Verfahrens.

Bester Weg zur Ausführung der Erfindung

Wie in der einzigen Figur veranschaulicht, ist eine Speicherzelle **10** bzw. ein Register zum Einschreiben bzw. Abspeichern von Daten x_i in Form eines Datenbitwortes über eine Verbindung **11** vorgesehen. Bevor jedoch der Operand x_i in die Speicherzelle **10** eingeschrieben wird, werden von einer Zufallszahlenquelle **12** Zufallszahlen erzeugt und über eine direkte Verbindung **14** in die Speicherzelle **10** eingeschrieben bzw. in dieser abgespeichert. Mit anderen Worten wird die Speicherzelle **10** mit einem Zufallswert r_i initialisiert. Alternativ zu der dargestellten Ausführungsform kann das Einschreiben des Zufallswertes r_i auch über die Verbindung **11** von einem Rechenwerk erfolgen, welches zuvor den Zufallswert von der Zufallszahlenquelle **12** erhalten hat.

Der Zeitpunkt dieser Vorinitialisierung ist beliebig wählbar und erfolgt bevorzugt nicht unmittelbar vor der krypto-

graphischen Operation. Zweckmäßigerweise erfolgt eine wiederholte Vorinitialisierung der Speicherbereich bzw. Register mit sich ändernden Zufallszahlen.

Werden die so vorinitialisierten Speicherbereiche bzw. Register im Zuge einer kryptographischen Operation mit Daten x_i geladen, ändert sich der Stromverbrauch nun lediglich abhängig von einer Differenz des Hamminggewichtes des Operanden x_i und des Hamminggewichtes der unbekannten Zufallszahl. Ausgehend von diesem zufälligen Differenzwert ist es nun nicht möglich, Angaben über die verwendeten Operanden bzw. Zwischenergebnisse abzuleiten.

Bezugszeichenliste

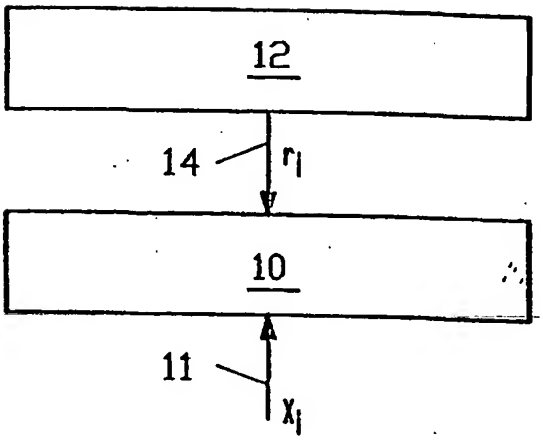
10 Speicherzelle/Register
11 Verbindung
12 Zufallszahlenquelle
14 Verbindung
Xi Daten
Ti Zufallswert

Patentansprüche

1. Verschlüsselungsverfahren, wobei wenigstens eine kryptographische Teiloperation von digital als wenigstens ein Datenbitwort in einer Speicherzelle (**10**) bzw. einem Register gespeicherten Daten ausgeführt wird, **dadurch gekennzeichnet**, dass vor dem Schreiben eines Datenbitwortes in eine Speicherzelle (**10**) in dieser ein Datenbitwort gespeichert wird, welches auf Zufallszahlen basierend erzeugt wird.
2. Verschlüsselungsverfahren nach Anspruch 1, dadurch gekennzeichnet, dass das auf Zufallszahlen basierende Bitwort von einem Rechenwerk in die Speicherzelle (**10**) geschrieben wird.
3. Verschlüsselungsverfahren nach Anspruch 1, dadurch gekennzeichnet, dass das auf Zufallszahlen basierende Bitwort über eine direkte Verbindung zwischen einer Zufallszahlenquelle (**12**) und der Speicherzelle (**10**) in letztere geschrieben wird.
4. Verschlüsselungsverfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das auf Zufallszahlen basierende Bitwort zeitlich beabstandet vor der kryptographische Teiloperation in der Speicherzelle (**10**) gespeichert wird.

Hierzu 1 Seite(n) Zeichnungen

Nummer: DE 199 36 890 A1
Int. Cl.[7]: G 06 F 12/14
Offenlegungstag: 6. April 2000



Fig